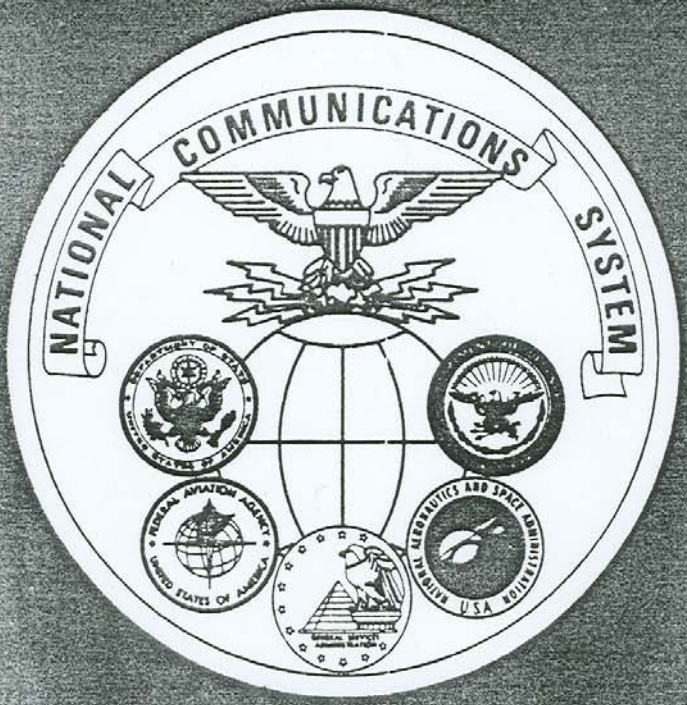
Federal Standard 1027 has been redesignated as Federal Information Processing Standards Publication (FIPS PUB) 140. Issued by the National Institute of Standards and Technology pursuant to Section 111(d) of the Federal Property and Administrative Services Act of 1949 as amended by the Computer Security Act of 1987, Public Law 100-235.

FIPS PUB 140

FEDERAL STANDARD 10

GENERAL SECURITY REQUIREMENTS FOR EQUIPMENT USING THE DATA ENCRYPTION STANDARD



ISSUED BY GENERAL SERVICES ADMINISTRATION

APRIL 14, 1

FED-STD-I027
April 14, 1982

FEDERAL STANDARD
TELECOMMUNICATIONS: GENERAL SECURITY REOUIREMENTS FOR EQUIPMENT USING THE DATA ENCRYPTION STANDARD

This standard is issued by the General Services Administration pursuant to the Federal Property and Administrative Services Act of 1949, as amended.

1. Scope

1.1 Description. This standard specifies the minimum general security requirements that are to be satisfied in implementing the Data Encryption Standard (DES) algorithm in a telecommunications environment. The DES itself specifies an algorithm used for cryptographically protecting certain U.S. Government information. (This algorithm is described in Federal Information Processing Standards Publication 46). The requirements defined in this standard affect the security of equipment implementing the DES algorithm. Other security requirements, which relate to the interface and interoperability of DES cryptographic equipment with associated terminal equipment (e.g., narrative text, automatic data processing, digital facsimile, digital voice, etc.), will be addressed in other Federal telecommunication standards.

1.2 Security Objectives. This standard addresses the following security objectives:

a. To prevent inadvertent transmission of plain text.

b. To prevent theft, unauthorized use, or unauthorized modification of DES cryptographic equipment while installed.

c. To prevent unauthorized disclosure or modification of key variables while in DES cryptographic equipment.

d. To provide interoperability between key variable loaders and DES cryptographic equipment, and facilitate the use of standardized keying material for U.S. Government applications of the DES algorithm.

e. To prevent data encryption when a critical cryptographic failure condition exists, and to generate an alarm upon detection of a critical cryptographic failure.

1.3 Purpose. This standard prescribes security requirements for implementation of the DES in telecommunication equipment an systems used by the departments and agencies of the U.S. Government.

1.4 Application. This standard applies to all DES cryptographic components, equipment, systems, and services procured (including lease) by U.S. Government departments and agencies for the encryption of digital information in the telecommunications environment. This includes stand-alone

DES cryptographic equipment as well as any Data Terminal Equipment and Data Circuit-terminating Equipment utilizing the DES algorithm for digital encryption. When DES cryptographic equipment is integrated into Data Terminal Equipment (DTE) or Data Circuit-terminating Equipment (DCE), this standard applies to those portions of the DTE or DCE design which implement the security requirements of this standard. The same degree of protection is required whether DES cryptographic equipment is in stand-alone units or is physically embedded in associated equipment. Guidance to facilitate the application of this standard, with respect to degradation of its security by improper implementation or use, will be provided for in a revision to Federal Property Management Regulation 41, Code of Federal Regulations 101-35.3.

1.5 Verifying Conformance. Procedures for verifying that DES cryptographic equipment conforms to this standard are available from the preparing activity.

1.6 Definitions and Conventions. The following definitions, conventions, and terminology apply in this standard.

a. Bypass: A condition which allows plain text to pass through equipment unaltered, with or without some delay.

b. DES: The Data Encryption Standard algorithm specified in Federal Information Processing Standards Publication 46.

c. DES Cryptographic Equipment: Equipment embodying one or more DES devices and associated controls, interfaces, power supplies, alarms, and the related hardware, software, and firmware used to encrypt, decrypt, authenticate, and perform similar operations on information.

d. DES Device: The electronic hardware part or subassembly which implements just the DES algorithm specified in Federal Information Processing Standards Publication 46, and which is validated by the National Bureau of Standards. ' ,

e. Initializing Vector (IV): A vector used in defining the starting point of an encryption process within a DES device.

f. Key Generator: A DES device plus those additional cryptographic functions required to implement: (I) a particular mode of encryption; (2) combining of plain text or cipher text with DES device output; (3) the initializing vector; and (4) associated alarms and self-testing. .

g. Key Variable: A 6'*-bit input to DES cryptographic equipment, with & bits used for parity checking and '6 bits used in the DES device for encryption or decryption. Unless otherwise stated, reference to a DES key variable means a key variable in its unencrypted form.

h. Key Variable Loader: An electronic, self-contained unit which is capable of storing at least one 64-bit DES key variable and transferring that key variable, upon request, into DES cryptographic equipment.

i. Message: A generic term used to describe, in the broadest sense, information to be transferred which' is represented by a digital sequence. This sequence should be numbered 1,2,. . .,N, where 1 represents the information unit transmitted first.

j. Physical Key: A device used to operate a mechanical lock.

k. Pseudorandom Binary Process: A deterministic technique for producing a sequence of binary digits which satisfy the statistical properties of a random bit stream.

l. S-Box: A nonlinear function which substitutes four output bits for six input bits within a DES device to make the DES algorithm a nonlinear process (see Federal Information Processing Standards Publication 46).

m. Zeroization: A method of erasing an electronically stored DES key variable by removing electrical power from the electronic storage, by overwriting that storage with an all ONEs or ZEROs pattern, or by otherwise irrevocably altering the contents of the DES key variable storage.

2. Referenced Documents

a. Federal Information Processing Standards Publication 46: DATA ENCRYPTION STANDARD. January, 1977. (Copies of this standard are available from the National Technical Information Service, U.S. Department of Commerce, 5285 Port Royal Road, Springfield, VA 22161.)

b. Federal Information Processing Standards Publication 81: DES MODES.OF OPERATION. December, 1980. (Copies of this standard are available from the National Technical Information Service, U.S. Department of Commerce, 5285 Port Royal Road, Springfield, VA 22161.)

c. Federal Standard 1031: TELECOMMUNICATIONS: GENERAL PURPOSE 37-POSITION AND 9-POSITION INTERFACE BETWEEN DATA TERMINAL EOUIPMENT AND DATA CIRCUIT-TERMINATING EQUIPMENT. (Copies of this standard are available from GSA, Specifications and Consumer Information Distribution Branch (WFSIS), Bldg. 197 (Washington Navy Yard), Washington, DC 20407).

d. Military Standard 4618: ELECTROMAGNETIC EMISSION AND SUSCEPTIBILITY REQUIREMENTS FOR THE CONTROL OF ELECTROMAGNETIC INTERFERENCE. (Copies of this standard are available from the Naval Publications and Forms Center, 5801 Tabor Avenue, Philadelphia, PA 19120.)

e. Military Standard 462: MEASUREMENT OF ELECTROMAGNETIC INTERFERENCE CHARACTERISTICS. (Copies of this standard are available from the Naval Publications and Forms Center, 5801 Tabor Avenue, Philadelphia, PA 19120.)

f. National Bureau of Standards Special Publication 500-20: VALIDATING THE CORRECTNESS OF HARDWARE IMPLEMENTATIONS OF THE NBS DATA ENCRYPTION STANDARD. September, 1980. (Copies of this publication are available as SN 003-003-01861-9 from the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402.)

g. National Bureau of Standards Special Publication 500-61: MAINTENANCE TESTING FOR THE DATA ENCRYPTION STANDARD. August, 1980. (Copies of this publication are available as SN 003-003-02225-0 from the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402.)

h. Proposed Federal Standard 1026: TELECOMMUNICATIONS: INTEROPERABILITY AND SECURITY REQUIREMENTS FOR USE OF THE DATA ENCRYPTION STANDARD IN THE PHYSICAL AND DATA LINK LAYERS OF DATA COMMUNICATIONS; dated June 1, 1981.

.

3. Requirements

3.1 Physical Security. DES cryptographic equipment shall be designed to restrict physical access to internally stored DES key variables and to deter theft, unauthorized use, or unauthorized modification of the equipment when installed. The level of physical security provided shall be such that unauthorized attempts at access or use wi1l either be unsuccessful or will have a high probability of being detected, during penetration or subsequent to penetration. The installation design must minimize the possibility of penetration which cannot be visually detected.

3.1.1 Locks. At least one lock shall be used to limit access to the key variable entry controls. When the Cipher Block Chaining mode is used and the Initializing Vector (IV) is externally entered into DES cryptographic equipment, access to the associated controls shall be limited by the same lock which protects the key variable entry controls. In addition, certain other controls shall be operated by means of a physical key-operated selection switch or shall be accessible only upon opening or removing a locked cover (see section 3.7). The physical key used to operate or access these controls shall be different from the physical key used to limit access to the key-variable entry controls. Note that "the two locks previously described may be used in conjunction with each other ("two person control") when protection against the possibility of unauthorized use is considered necessary. All locks shall be of the pick-resistant variety (MEDECO or equivalent).

3.1.2 Mounting. A means shall be provided to protect against theft and substitution of DES cryptographic equipment when installed (with or without a key variable present). A solution such as a mounting mechanism accessible only from the interior of the locked equipment shall be used to deter removal of the equipment by any means other than determined force.

3.1.3 Standby Periods. DES cryptographic equipment shall be designed so that operating personnel can conveniently make it inoperable (while retaining the key variable) during periods when the equipment is in standby, and not in operation. This shall be implemented in such a manner as to prevent unauthorized use, for example, by reapplication of power. Once placed in standby, equipment shall not be capable of being restored to operation without the operation of at least one lock.

3.1.4 Equipment Enclosure. DES cryptographic equipment enclosures shall be designed such that a physical lock must be operated in order to disassemble the equipment to an extent that would permit undetectable access to internal circuitry. Also, all holes placed in the outside surface of the equipment during manufacture shall be located such that undetectable access to key variable storage and processing circuitry, as well as undetectable disassembly of the equipment, are not possible using these holes.

3.2 Key Variables. The security provided by DES cryptographic equipment is dependent upon the DES key variable. The same DES key variable must be inserted into equipment in a link or network to make a grouping of equipment cryptographically unique and compatible. A DES key variable consists of 64 bits (Kl through K64), 56 bits of which are randomly or pseudorandomly derived and 8 bits of which are odd parity check bits. Each bit of odd parity is computed individually on its

preceding seven-bit group of random or pseudorandom bits according to the convention shown in table 1.

3.2.1 Key Variable Entry. Two approved methods of entering unencrypted DES key variables into DES cryptographic equipment are described below. All DES cryptographic equipment shall utilize at least one of these two methods of key variable entry. This is required to perform one or more of the following: (I) to enter DES key variables for normal encryption and decryption, (2) to provide the capability to enter a key variable to decrypt encrypted and electronically transmitted key variables, and (3) to facilitate maintenance. Ciphertext output shall be inhibited during transfer of key variables into DES devices. A means of permitting operating personnel to either conveniently correct errors made during manual key variable entry or to reenter the entire key variable shall be provided. When a DES key variable is assembled into a single 64-bit sequence, the bits shall be ordered in the following manner K I,K2. . . ,K64. This numbering corresponds to the numbering of key variable bits defined in Federal Information Processing Standards Publication 46.

3.2.1.1 Method 1. DES cryptographic equipment may contain an integral capability to manually enter DES key variables from printed form. The printed DES key variables shall consist of a sequence of 16 symbols (V1, V2, . ., V16) entered starting with the left-most symbol (V1). Each printed symbol represents a four-bit binary word corresponding to four bits of the DES key variable, as defined in table 2. Manual entry can be accomplished by any technique which provides relatively easy, reliable loading (e.g., keyboard, rotary switches, thumbwheel switches, etc.). If a DES key variable is displayed electrically or mechanically, all visual residue of the DES key variable shall be removed automatically after it is accepted as valid (see section 3.2.4).

3.2.1.2 Method 2. DES cryptographic equipment may accept key variables in electronic form from an externally connected key variable loader in accordance with the electrical and mechanical Interface requirements of this standard. When the 64-bit DES key variable sequence is transferred serially, the order of transfer is as listed in section 3.2.1, with K1 being the first bit transferred. After a DES key variable has been entered into a key variable loader and verified by the key variable loader (successful parity check), there shall be no visual or mechanical residue of the key variable available to a person having access to the key variable loader. The key variable loader shall have a zeroize capability controlled by operating personnel.

3.2.1.2.1 Key Variable Transfer Operation. Electronic key variable transfer into DES cryptographic equipment from a key variable loader is initiated by the DES cryptographic equipment under control of operating personnel. Operating personnel shall initiate the key variable transfer by some manual action to the DES cryptographic equipment which will result in a REQUEST indication being sent by the DES cryptographic equipment to the key variable loader. Upon receipt of REQUEST indication, the key variable loader will provide a 64-bit serial key variable on the DATA circuit and an associated 64 cycles of clock on the CLOCK circuit. The timing involved in this DES key variable transfer is shown in figure 1.

3.2.1.2.2 Interface Circuits. The DES key variable transfer interface shall consist of nine circuits: GROUND, REQUEST, DATA, CLOCK, VDD, and four undesignated circuits. The functional relationship of the REOUEST, DATA, and CLOCK circuits is shown in figure 1.

a. GROUND. This circuit is connected to logic ground within DES cryptographic equipment. In many equipment, this circuit will also be connected to chassis ground, internal to the equipment.

b. REQUEST. This circuit is normally OFF (high). It turns ON (low) as a result of an action by operating personnel to initiate a key variable transfer. REOUEST is generated by DES cryptographic equipment.

c. DATA. In response to a REQUEST Indication, the DATA circuit conveys the 64 bits of DES key variable to the DES cryptographic equipment. The DATA circuit may also be used, under control of the undesignated circuits, for other purposes. DATA is generated by the key variable loader.

d. CLOCK. In response to REQUEST indication, the CLOCK circuit sends 64 clock cycles synchronously, and in a specified phase relationship with respect to the key variable bits on the DATA circuit. The CLOCK circuit may also be used for other purposes, under control of the undesignated circuits. CLOCK is generated by the key variable loader. DES cryptographic equipment shall respond to only the first 64 clock cycles (and ignore any additional clock cycles) associated with a given DES key variable transfer in response to a REQUEST indication.

e. VDD. This circuit is connected to a regulated 5+/-0.5 volt power supply within the DES cryptographic equipment. VDD provides a positive logic voltage reference for key variable loaders with floating ground and negative internal logic (such as the KOI-18). .

f. Undesignated Circuits. Use of the four undesignated circuits is optional, and they can be used for any function associated with key variable management and/or equipment control. The electrical parameters of these undesignated circuits, if used, must conform to the general electrical requirements contained in section 3.2.1.2.3 and table 3 of this standard. Specifically, undesignated output and input circuits shall meet the requirements of sections 3.2.1.2.3.a and 3.2.l.2.3.b of this standard, respectively. DES cryptographic equipment shall be capable of accepting key variables from key variable loaders which do not have or use the undesignated circuits.

3.2.1.2.3 Electrical Interface Characteristics. The electrical characteristics in this section apply at the DES cryptographic equipment connector used for electronic key variable entry. All electrical measurements are with respect to GROUND. Logic levels for the circuits are defined in table 3 and are compatible with commercially available 4000-series CMOS digital integrated circuits operated from a five-volt power source. The logic levels in table 3 shall be met for the following load conditions:

a. REQUEST. The output voltage levels in table 3 shall be met when driving loads greater than 50 kohms with shunt capacitances less than 200 pF. .

b. DATA and CLOCK. These input circuits shall function properly when the input voltage levels in table 3 are applied to input loads greater than 200 kohms with shunt capacitances less than 50 pF.

3.2.1.2.4 Mechanical Interface Characteristics. DES cryptographic equipment shall be physically connected to a key variable loader via a cable, not to exceed one meter in length, using the type of nine-position connector specified in Federal Standard 1031 (based upon Electronic Industries Association standard RS-449). DES cryptographic equipment shall provide, via front panel access (under lock control), the female nine-position connector with latching blocks, for electronic key variable entry. The cable from the key variable loader shall use a matching male nine-position connector: one capable of latching. The position assignments for this connector are contained in table 4.

3.2.2 Parity. The parity of unencrypted DES key variables shall be verified during entry, whether manual or electronic, and during any subsequent transfer within DES cryptographic equipment, to ensure that no accidental single-bit modification of a key variable has occurred. Each group of eight bits shall be of odd parity, as defined in Federal Information Processing Standards Publication 46.

3.2.3 Zeroization. Any detected attempt to gain access to the internal components of DES cryptographic equipment, through disassembly of the equipment (e.g., removal of case), shall automatically zeroize the key variable and, in the Cipher Block Chaining mode, the Initializing Vector. All key variable storage locations, except those containing test key variables and encrypted key variables, must be capable of being zeroized. The ability to inhibit the zeroization feature shall be provided in the interior of equipment for maintenance. This inhibit feature must not be accessible until the equipment has been opened for maintenance. A means shall be provided to automatically disengage the internal inhibit feature and zeroize the maintenance test key variable in the DES device before DES cryptographic equipment is returned to the operational mode. A means shall also be provided to ensure that DES cryptographic equipment is not able to encrypt and decrypt when in the zeroized state.

3.2.4 Key Variable Storage. After initial key loading, all unencrypted key variables shall be stored inside DES cryptographic equipment, in order to receive the protection associated with the security requirements of this standard. A means must be provided to assure that unencrypted key variables cannot visually or electrically be read out of DES cryptographic equipment. If key variables are read out of DES cryptographic equipment for purposes of transmission, they must be encrypted first. Key variables must be stored in erasable electronic storage (e.g., random access memory, shift registers, the DES device, etc.). DES cryptographic equipment must also have the ability to maintain their key variables whenever primary power is interrupted. Except for key variables residing in "final" locations (actual use or protection against power interruption) within DES cryptographic equipment, the appearance of a key variable in any intermediate storage location within DES cryptographic equipment must be only temporary (e.g., as a part of the key variable entry or testing process) and all such temporary storage locations must be zeroized upon transfer of the key variable to one of its "final" locations. The DES key variable, when routed internally within DES cryptographic equipment, shall be routed in such a manner as to prevent external access to the key variable, either inadvertently or due to the single failure of an electronic component.

3.3 Initializing Vector (JV). Initializing vectors can be produced using the DES algorithm, a key variable, and input data generated internally; or they can be derived from another random or pseudorandom source. New IV's shall be derived such that all possible IV's (N bits long) are equally likely (i.e., have a probable occurrence of 2-N). A means shall be provided to assure the introduction of new initializing vectors following the loading of new key variables, return of primary power after a power interruption (except for in the Cipher Block Chaining: encryption mode), or upon start-up after the DES device has been zeroized or reset (e.g., when the device is first brought into service or after a battery change). The following IV requirements also apply:

a. An IV shall be used to initiate every ciphertext chain (see proposed Federal Standard 1026).

b. When the Cipher Feedback encryption mode is used, the IV shall contain a minimum of 48 bits, may be transmitted unencrypted, and shall be newly generated for every ciphertext chain.

c. When the Cipher Block Chaining encryption mode is used, the IV shall contain 64 bits, shall be encrypted prior to transmission, and need be newly generated only when a new key variable is entered into a DES device.

d. When the Output Feedback encryption mode is used, the IV shall contain 64 bits, and may be transmitted unencrypted.

3.3.1 Initializing Vector Retention. Except in the Cipher Block Chaining mode, the last initializing vector used should be retained in storage during an interruption of primary power, if it is to be used to generate a new initializing vector upon resumption of operation. In the Cipher Block Chaining mode, the initial IV should be retained for reuse to eliminate the need to retransmit it securely.

3.4 Encryption Function and Alarms

3.4.1 Modes. Four modes of implementing the DES have been approved. These modes are described in detail in Federal Information Processing Standards Publication 81. The Cipher Feedback and Cipher Block Chaining modes are intended for encryption of narrative text and Automatic Data Processing (ADP) data, for transmission over communications channels. The Output Feedback mode is intended for applications where error extension due to encryption/decryption cannot be tolerated. The Electronic Codebook mode is approved for the encryption and decryption of Data Encrypting Keys (DEK's) and IV's, for transmission over telecommunication systems. Use of the Electronic Codebook mode for other purposes, and use of other encryption/decryption modes, shall be approved by the responsible U. S. Government agency, as designated in section 1.4.

3.4.2 Encryption Tests. DES cryptographic equipment shall be designed to provide for automatic testing of the encryption function, in addition to any other self-testing methods that are provided. To ensure that DES cryptographic equipment is not used to encrypt messages after it has failed, one of the following two methods shall be employed:

3.4.2.1 Method I. Two DES key generators shall be used to do the same encryption of plaintext data. Their outputs shall be compared. Any difference between the outputs shall generate an alarm and shall cause the ciphertext output to immediately cease until operating personnel eliminate the error condition, or take such other action as may be prescribed by approved operational procedures. A means to automatically test the comparator circuits and associated inhibiting circuits (e.g., cause an intentional error) shall be provided.

3.4.2.2 Method 2. An acceptable alternative to the continuous comparison of the outputs of two key generators operating in parallel is the use of a single key generator whose integrity is verified by both of the following two tests (or just the S-box test if it is run at the frequency prescribed for the DES checkword test). These tests do not strictly meet the security objective stated in section 1.2.e, but they do serve to limit the transmission of data under critical failure conditions.

3.4.2.2. S-Box Test. This test consists of loading one or more known key variables (test variables) and one or more known 64-bit inputs into the transmit DES device and operating the DES key generator until all S-box entry combinations for each S-box have been applied. The final output(s) are then compared with all 64 bits of the known correct result(s) (determined previously, off-line, and stored in the equipment). If they fail to compare, an alarm shall be automatically generated and all ciphertext output shall be inhibited until operating personnel eliminate the error condition, or take such other action as prescribed by approved operating procedures. A means of automatically testing

the comparator circuits and associated inhibiting circuits (i.e., cause an intentional error) shall be provided. (Descriptions of several S-box tests are contained in National Bureau of Standards Special Publications 500-20 and 500-61).

3.4.2.2.2 DES Checkword Test. After a new DES key variable is loaded into the DES cryptographic equipment, and after the S-box test has been performed, a known 64-bit input word is encrypted in the new key variable and the resulting 64-bit checkword is stored. This checkword shall be retained in storage and used until the new key variable is superseded. The DES checkword test consists of encrypting the known 64-blt input word in the current DES key variable and comparing the result with all 64 bits of the checkword. If they fail to compare, an alarm shall be automatically generated and the ciphertext output of the DES cryptographic equipment shall be inhibited until operating personnel eliminate the error condition, or take such other action as prescribed by approved operating procedures. A means of automatically testing the comparator circuits and associated inhibiting circuits (i.e., cause an intentional error) shall be provided. The S-box test may be used in place of the DES checkword test, if advantageous. When this is done, the S-box test must be run at the frequency prescribed for the DES checkword test.

3.4.2.3 Frequency of Testing. When two DES devices are operated in parallel (see section 3.4.2. I), the self-checking is continuous. When only one device is used with the S-box and DES checkword tests (see section 3.4.2.2), testing of the DES device is not continuous. In such an instance, the S-box test shall be accomplished to ensure correct operation of the device at the time of key variable entry, and the DES checkword test shall be accomplished prior to each use of an initializing vector. Automatic testing of the comparator circuits used in implementing method 1 or 2 (see sections 3.4.2.1 and 3.4.2.2) shall be performed when practical, but no less frequently than upon each DES key variable entry into the DES device.

3.4.3 Other Tests

3.4.3.1 Control Field Recognition In automatic data processing and narrative text telecommunication applications, provision shall be made to verify that stand-alone DES cryptographic equipment can recognize implicit or explicit control fields signaling the start of encryption (e.g., START OF TEXT). A means of automatically testing the above-mentioned functions (i.e., cause intentional errors) shall be provided. When the control field recognition functions are tested, failure of DES cryptographic equipment to recognize and act upon these fields shall inhibit operation in the secure mode and generate an alarm. Provision may be made internal to DES cryptographic equipment to conveniently override this feature to facilitate maintenance. When the DES cryptographic equipment function is integrated into Data Terminal Equipment (DTE), and data is encrypted as a consequence of being processed within the DTE, the requirement to check the ability to recognize these control fields may not be necessary. In these cases, where the DTE provides but does not check the control field recognition function(s), the DTE design shall assure that data intended for encryption will always be encrypted and will never be transmitted unencrypted.

3.4.3.2 Chain Identification (CID), Manipulation Detection Code (MDC) and Message Authentication Code (MAC). In systems which utilize the CID, MDC or MAC fields, an alarm shall be generated when the received MDC, CID, or MAC mismatches (i.e., does not compare) with the expected value. When DES cryptographic equipment is generating and checking the CID, MDC, or MAC fields and mismatch occurs, the DES cryptographic equipment shall generate an alarm. CID's shall not be repeated for a given key variable period. When DES cryptographic equipment is generating the CID, the equipment shall generate an alarm when the CID counter reaches its

maximum value. In full-duplex and multidrop applications, provision must be made to assure that CID's are not duplicated by the various terminals. Details of the CID, MDC, and MAC fields are described in proposed Federal Standard 1026. DES cryptographic equipment (or a DTE or DCE providing the CID, MDC, or MAC functions) must also be capable of testing the comparator(s) used to compare a received CIO, MDC, or MAC with the expected or locally derived value (e.g., cause an intentional error). If a CID, MDC, or MAC comparator fails its test, an alarm shall be generated, and operation in the secure mode shall cease.

3.4.3.3 Other Ciphertext-Inhibit Tests. In addition to the conditions described in section 3.4.2 and previous paragraphs in section 3.4.3, ciphertext output of DES cryptographic equipment is also inhibited by: (a) transfer of a DES key variable into a DES device, (b) zeroization of DES cryptographic equipment, (c) use of the test mode, and (d) use of a DES device for a function other than the encryption of plaintext data (e.g., generating an IV, computing an MAC). DES cryptographic equipment shall be capable of testing that the conditions described in (a), (b), (d, and (d) above are capable of inhibiting ciphertext output.

3.4.3.4 Parity Check Verification. DES cryptographic equipment and key variable loaders shall be capable of testing that DES key variables with improper parity can be detected.

3.4.3.5 Frequency of Testing. The ability of DES cryptographic equipment (and DTE's or DCE's providing the CIO, MDC, or MAC functions) to recognize the control fields described in section 3.4.3.1, to perform the comparisons described in section 3.4.3.2, and to generate an alarm when an error or mismatch resulting from the use of these functions is detected, shall be checked at the same frequency required for the DES checkword test (see section 3.4.2.3). The MAC comparator shall be checked once per authenticated message. The tests described in sections 3.4.3.3 and 3.4.3.4 shall be performed at the same frequency as the S-box test.

3.5 Fail-Safe Design Requirements. DES cryptographic equipment design shall not contain potential single failures which could compromise DES key variables, or affect the initialization process. Specifically, DES cryptographic equipment design shall not permit potential single failure conditions which could result in: (1) transmission of the key variable, or any portion thereof, or (2) transmission in depth (reuse of the same IV) due to faulty or insufficient randomization. When firmware techniques are used to control the cryptographic functions described above, sufficient safeguards shall be incorporated to ensure proper operation of the firmware. (Note: Other critical areas (such as plain text handling, alarms, and alarm checks) that may be affected by undetected failures also deserve special consideration in design).

3.6 Test Mode. DES cryptographic equipment shall have a test mode which, when used, will assure that the equipment is operating as intended. At a minimum, the test mode shall perform an S-box test, when using Method 2 (see section 3.4.2.2), and test all security alarm circuitry. In the test mode, a test DES key variable(s) shall be used. The ciphertext output of DES cryptographic equipment shall be inhibited while in the test mode. However, a means may be provided for maintenance personnel to override the ciphertext output inhibit feature from inside the equipment. If the ciphertext inhibit override feature is implemented, a means shall be provided to automatically disengage the ciphertext inhibit override before DES cryptographic equipment is returned to the operational mode. DES cryptographic equipment shall prevent the test key variable from being used for encryption/decryption of actual plaintext/ciphertext data.

3.7 Control Functions. DES cryptographic equipment shall provide for the following controls under the conditions listed:

NAME	FUNCTION	CONDITIONS
POWER ON/OFF	Turns primary power (and internal battery) ON or OFF and causes zeroization of critical storage when in the OFF position. (See section 3.9.)	Optional feature. Lock not required.
STANDBY MODE	Provides the capability to render the DES device inoperable during unattended periods, without zeroizing the key variable. (See section 3.1.3.)	Required when equipment is not in continuous 24-hour a day operation. Must be under control of a lock.
ALARM RESET	Provides the capability to clear alarms after a fault has been corrected by repeating those security checks which could have generated the alarm condition. Performance of the security checks must be successful (i.e., the condition causing the alarm must have been corrected) before the alarm state can be exited. The ciphertext output shall be inhibited until the alarm state is exited.	Required on all equipment. Must be under control of a lock.
TEST MODE	Causes DES cryptographic equipment to perform tests contained in section 3.6 of this standard.	Required on all equipment. Must be under control of a lock.
LAMP TEST	Provides assurance that indicators are operable.	Optional feature. No lock required.
KEY VARIABLE ENTRY	Provides for external entry of DES key variable(s), either manually or automatically. (This does not include "down-line loading".) Ciphertext output shall be inhibited during entry of the key variables if the DES key variables are automatically placed in a DES device as a result of entry.	Required if external key variable entry devices are used. (See section 3.1.1)
BYPASS MODE	Provides the capability for bypassing the DES device and transmitting plain text when DES cryptographic equipment is in an alarm condition or other malfunction condition.	Optional feature. Must be under control of a lock.

SECURE MODE	Provides capability to transmit and receive cipher text.	Optional feature. Must be under control of a lock.
ZEROIZE	Provides capability to zeroize all unencrypted key variables (and IV in CBC mode).	Required feature on all equipment. No lock required.

NOTE: It is not necessary to provide individual locks for each control function. They may, for instance, be collocated (within the constraints of section 3.1.1 of this standard) behind a locked cover or gated by a physical key switch.

3.8 Status Indicators. DES cryptographic equipment shall provide for display of the following indications of status under the conditions listed below.

NAME	FUNCTION	CONDITIONS
POWER ON	Indication that proper electrical power is available for equipment operation.	Required only when power ON/OFF switch is used.
DES BYPASS	Indication that the equipment is not in the encipher/decipher state.	Required when BYPASS control is implemented.
TEST	Indication that DES cryptographic equipment is in a test mode, as opposed to an operational mode.	Required on all equipment.
BATTERY	Indicates whether the internal battery is operating properly and is capable of retaining critical storage.	Required when a battery is used as a backup energy source.
ALARM	Indication that an error in operation of the DES cryptographic equipment has occurred or that attempted tampering has been detected. Ciphertext output must be automatically and immediately disabled when an alarm occurs, if not in the bypass condition.	Required on all equipment.
AUDIBLE ALARM	Same as ALARM.	Optional feature. Not a front panel indicator. A dry contact relay type of interface shall be used and should be available on the rear of the equipment.
PARITY	Indication that an error in parity has occurred during DES key variable entry or during internal transfer of the key variable. Further internal key variable transfers shall be inhibited until the condition which caused the error is corrected and a correct key variable has been entered.	Required on all equipment.

3.9 Retention of Critical Storage. Critical storage (e.g., key variable final storage location(s), CID's, IV's, and test data) in DES cryptographic equipment shall be retained during primary power interruptions. DES cryptographic equipment shall have a means of determining whether critical storage has been properly maintained during interruption of primary power.

3.10 EMI/EMC Requirements. DES cryptographic equipment shall be designed and constructed to meet the Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC) requirements of MIL-STD-461B for class A-3 equipment. Good EMI design practices should be followed in all aspects of the DES cryptographic equipment design. DES cryptographic equipment shall comply with the test requirements of MIL-STD-462 as specified below in all operating modes:

TEST	REQUIREMENT
CE01	Narrowband measurements only required; limits specified in figure 4-1, curve 1, for Direct Current (DC) and Alternating Current (AC) power leads and control and signal leads.
CE03	Figure 4-4, curve 1, broadband, and figure 4-3, curve 1, narrowband, apply for DC and AC power leads and control and signal leads.
RE01	Figure 4-11 applies with the following modification: The limit from 3 kHz to 50 kHz shall be 60 dB above 1 pT.
RE02	Figure 4-12, narrowband, and figure 4-13, broadband, apply.

4. Deviations and Changes to Federal Standard 1027. When a Federal Agency considers that this standard does not provide for its essential needs, a statement citing inadequacies shall be sent in duplicate to the General Services Administration (C), Washington, DC 20405. The General Services Administration and the preparing activity, in accordance with Federal Property Management Regulations 41 CFR 101-29.3, will determine the appropriate action to be taken and will notify the agency. Manufacturers and suppliers may contact the preparing activity for information regarding precedures for requesting approval for equivalent methods to be used, to meet the requirements of this standard. Supplementary guidance concerning requests for such approval is being provided in a revision to Federal Property Management Regulation 41, Code of Federal Regulations 101-35.3.

PREPARING ACTIVITY:

Communications Security Organization
National Security Agency
9800 Savage Road
Fort George G. Meade, MD 20755

MILITARY INTERESTS:

Military Coordinating Activity
NSA -- NS

Custodians
Army -- SC
Navy -- EC
Air Force -- 02

Review Activities
Army -- AD, CR
Navy -- AS, OM
Air Force -- 90
DCA -- DC
TRI-TAC -- TT
DLA -- DH

User Activities
Navy -- SH, MC

This document is available from the General Services Administration (GSA), acting as agent for the Superintendent of Documents. A copy for bidding and contracting purposes is available from GSA Business Centers. Copies are for sale at the GSA Specification Unit (WFSIS), Room 6039, 7th and D Streets S.W., Washington, D.C. 20407; telephone (202) 472-2205. Please call in advance to arrange for pickup service.

Parity Bit	Key Variable Bits Checked By Parity Bit
K8	K1, K2, K3, K4, K5, K6, K7
K16	K9, K10, K11, K12, K13, K14, K15
K24	K17, K18, K19, K20, K21, K22, K23
K32	K25, K26, K27, K28, K29, K30, K31
K40	K33, K34, K35, K36, K37, K38, K39
K48	K41, K42, K43, K44, K45, K46, K47
K56	K49, K50, K51, K52, K53, K54, K55
K64	K57, K58, K59, K60, K61, K62, K63

TABLE 1

Printed Symbol	DES Key Variable Bits Significant ◀ Most Least ▶
V1	K1, K2, K3, K4
V2	K5, K6, K7, K8
V3	K9, K10, K11, K12
V4	K13, K14, K15, K16
V5	K17, K18, K19, K20
V6	K21, K22, K23, K24
V7	K25, K26, K27, K28
V8	K29, K30, K31, K32
V9	K33, K34, K35, K36
V10	K37, K38, K39, K40
V11	K41, K42, K43, K44
V12	K45, K46, K47, K48
V13	K49, K50, K51, K52
V14	K53, K54, K55, K56
V15	K57, K58, K59, K60
V16	K61, K62, K63, K64

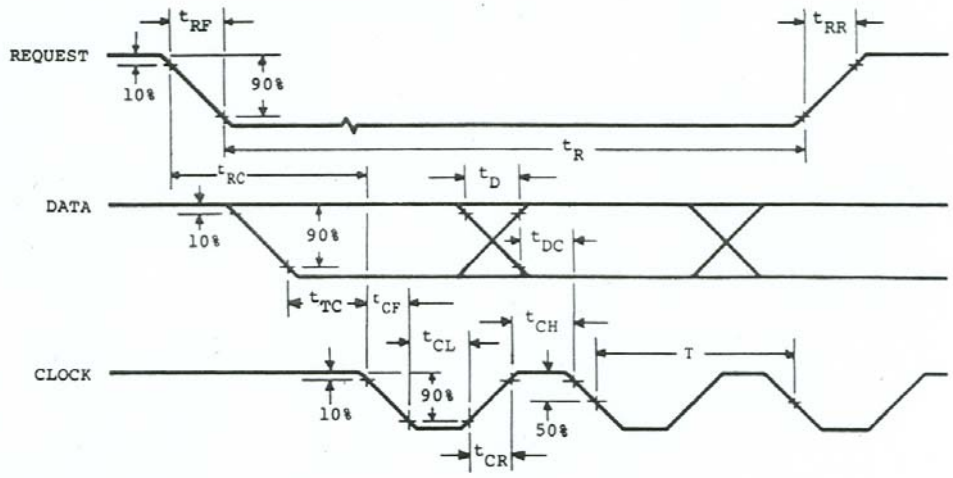
TABLE 2

Logic Level	Input (Volts)		Output (Volts)	
	Maximum	Minimum	Maximum	Minimum
HIGH (Logical ONE)	5.0	4.0	5.0	4.6
LOW (Logical ZERO)	1.0	-2.0	0.5	0

TABLE 3

Position	Function
1	GROUND
2	UNDESIGNATED
3	REQUEST
4	UNDESIGNATED
5	DATA
6	CLOCK
7	UNDESIGNATED
8	UNDESIGNATED
9	VDD

TABLE 4



Time	Minimum	Maximum
T	253 µs (3960 Hz)	781 µs (1280 Hz)
t_{CH}	100 µs	--
t_{CL}	100 µs	--
t_{CF}	--	20 µs
t_{CR}	--	20 µs
t_{DC}	100 µs	--
t_{RC}	300 µs	10 ms
t_{RF}	--	40 µs
t_{RR}	--	40 µs
t_R	10 ms*	--
t_{TC}	100 µs	--
t_D	--	20 µs

* NOTE: Or until the first data bit is received

FIGURE 1